IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: DANY MARGALIT, et al

For: CLASSIFYING DIGITAL OBJECT SECURITY CATEGORY

Attorney Docket No.:U 013682-7

Assistant Commissioner for Patents
Washington, D.C. 20231

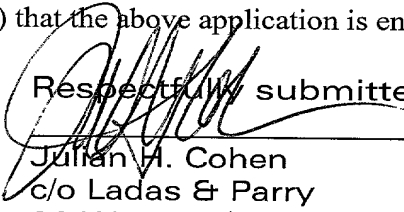## WRITTEN ASSERTION OF SMALL ENTITY STATUS

This is written assertion on the basis of:

☐ personal knowledge;

☐ applicant's letter of _____;

☐ applicant's agent's letter of OCTOBER 18, 2001; or

☐ other _____

by a practitioner (not necessarily of record) that the above application is entitled to small entity status and, therefore, fees.

Respectfully submitted,

Julian A. Cohen
c/o Ladas & Parry
26 West 61st Street
New York, N.Y. 10023

CERTIFICATION UNDER 37 C.F.R. 1.8(a) and 1.10*
*(When using Express Mail, the Express Mail label number is **mandatory**;*
Express Mail certification is optional.)
I hereby certify that, on the date shown below, this correspondence is being:
MAILING

☒ deposited with the United States Postal Service in an envelope addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

37 C.F.R. 1.8(a)	**37 C.F.R. 1.10***
☐ with sufficient postage as first class mail.	☒ as "Express Mail Post Office to Address" Mailing Label No. EV/011018807 US **(mandatory)**

TRANSMISSION

☐ transmitted by facsimile to the Patent and Trademark Office.

Date: October 22, 2001

Signature

__CONNIE YANNOTTI__
(type or print name of person certifying)

WARNING: *Each paper or fee filed by "Express Mail" **must** have the number of the "Express Mail" mailing label placed thereon prior to mailing. 37 C.F.R. 1.10(b).*

*"Since the filing of correspondence under § 1.10 without the Express Mail mailing label thereon is an oversight that can be avoided by the exercise of reasonable care, requests for waiver of this requirement will **not** be granted on petition." Notice of Oct. 24, 1996, 60 Fed. Reg. 56,439, at 56,442.*

Written Assertion of Small Entity Status **7-10a**

42122AL7.doc   14/08/01

FIELD OF THE INVENTION

[0001]   The present invention relates to computer systems and methodologies generally and more particularly to systems and methodologies for detecting the presence of malicious content.

BACKGROUND OF THE INVENTION

[0002]   There exist various techniques for detecting the presence of malicious content. The following U.S. patents are believed to represent the current state of the art: 5,473,769; 5,696,822; 5,991,774.

SUMMARY OF THE INVENTION

[0003]   The present invention seeks to provide an improved system and methodology for detecting the presence of malicious content.

[0004]   There is thus provided in accordance with a preferred embodiment of the present invention a method of detecting malicious content. The method includes examining at least two characteristics of a digital object, analyzing the characteristics to determine whether there exists a mismatch therebetween and upon determining the existence of a mismatch, classifying the digital object as a digital object possibly containing malicious content.

[0005]   There is also provided in accordance with a preferred embodiment of the present invention a method of detecting malicious content. The method includes obtaining information relating to at least two characteristics of a digital object, analyzing the information to categorize the digital object into at least two categories, comparing the categories to decide whether there exists a mismatch therebetween and upon determining the existence of a mismatch, classsifying the digital object as a digital object possibly containing malicious content.

[0006]   There is provided in accordance with yet another preferred embodiment of the present invention a method of detecting malicious content. The method includes examining at least two characteristics of a digital object, each of which characteristics may be selected by a creator of the digital object independently of selection of another characteristic. analyzing the characteristics to determine whether there exists a

1

mismatch therebetween and upon determining the existence of a mismatch, classifying the digital object as a digital object possibly containing malicious content.

[0007]   There is further provided in accordance with a preferred embodiment of the present invention a system for detecting malicious content. The system includes a digital object examiner, which examines at least two characteristics of a digital object, a characteristics mismatch detector, which analyzes the characteristics to determine whether there exists a mismatch therebetween and a digital object classifier, operating upon the determination of the existence of a mismatch, for classifying the digital object as a digital object possibly containing malicious content.

[0008]   There is also provided in accordance with another preferred embodiment of the present invention a system for detecting malicious content. The system includes a digital object information obtainer, obtaining information related to at least two characteristics of a digital object, a characteristic based categorizer, categorizing the information into at least two categories, a categories mismatch detector, analyzing the categories to determine whether there exists a mismatch therebetween and a digital object classifier, operating upon determining the existence of a mismatch, classifying the digital object as a digital object possibly containing malicious content.

[0009]   There is further provided in accordance with yet another preferred embodiment of the present invention a system for detecting malicious content. The system includes a digital object examiner, for examining at least two characteristics of a digital object, each of the characteristics may be selected by a creator of the digital object independently of selection of another characteristic, a characteristics mismatch detector, analyzing the characteristics to determine whether there exists a mismatch therebetween and a digital object classifier, operating upon determining the existence of a mismatch, classifying the digital object as a digital object possibly containing malicious content.

[0010]   Further in accordance with a preferred embodiment of the present invention the malicious content includes malicious code. Additionally or alternatively, the malicious content includes the masqueraded content.

[0011]   Still further in accordance with a preferred embodiment of the present invention at least one of the characteristics is selected from a set consisting of: header information, file content, file name extension and file icon.

2

[0012]   Preferably, the digital object is selected from a set consisting of: a file, an e-mail attachment, a web page and a storage medium.

[0013]   Additionally in accordance with a preferred embodiment of the present invention the digital object includes a file, an e-mail attachment, a web page and/or a storage medium.

[0014]   Still further in accordance with a preferred embodiment of the present invention the characteristics include header information and file content, header information and file name extension, header information and file icon, file content and file icon, file name extension and file icon and/or file name extension and file content.

[0015]   Additionally in accordance with a preferred embodiment of the present invention the digital object examiner includes a digital object examiner server subsystem, the characteristics mismatch detector includes a mismatch detector server subsystem and the digital object classifier includes a mismatch detector server subsystem.

[0016]   Still further in accordance with a preferred embodiment of the present invention the digital object examiner includes a digital object examiner client subsystem, the characteristics mismatch detector includes a mismatch detector client subsystem and the digital object classifier includes a mismatch detector client subsystem.

[0017]   Further in accordance with a preferred embodiment of the present invention the digital object examiner includes a digital object examiner gateway subsystem, the characteristics mismatch detector includes a mismatch detector gateway subsystem and the digital object classifier includes a mismatch detector gateway subsystem.

[0018]   Preferably, the digital object examiner is selected from a set consisting of: a digital object examiner server subsystem, a digital object examiner client subsystem and a digital object examiner gateway subsystem.

[0019]   The digital characteristics mismatch detector is preferably selected from a set consisting of: a characteristics mismatch detector server subsystem, a characteristics mismatch detector client subsystem and a characteristics mismatch detector gateway subsystem.

3

[0020] The digital object classifier is preferably selected from a set consisting of: a digital object classifier server subsystem, a digital object classifier client subsystem and a digital object classifier gateway subsystem.

[0021] Further in accordance with a preferred embodiment of the present invention the digital object examiner includes a digital object examiner client subsystem. the characteristics mismatch detector includes a mismatch detector client subsystem and the digital object classifier includes a mismatch detector client subsystem.

[0022] Still further in accordance with a preferred embodiment of the present invention the digital object information obtainer includes a digital object information obtainer server subsystem, the characteristic based categorizer includes a characteristic based categorizer server subsystem, the categories mismatch detector includes a mismatch detector server subsystem and the digital object classifier includes a mismatch detector server subsystem.

[0023] Additionally in accordance with a preferred embodiment of the present invention the digital object information obtainer includes a digital object information obtainer client subsystem, the characteristic based categorizer includes a characteristic based categorizer client subsystem, the categories mismatch detector includes a mismatch detector client subsystem and the digital object classifier includes a mismatch detector client subsystem.

[0024] Still further in accordance with a preferred embodiment of the present invention the digital object information obtainer includes a digital object information obtainer gateway subsystem, the characteristic based categorizer includes a characteristic based categorizer gateway subsystem, the categories mismatch detector includes a mismatch detector gateway subsystem and the digital object classifier includes a mismatch detector gateway subsystem.

[0025] Preferably, the digital object information obtainer is selected from a set consisting of: a digital object information server subsystem, a digital object information client subsystem and a digital object information gateway subsystem.

[0026] The characteristic based categorizer is preferably selected from a set consisting of: a characteristic based categorizer server subsystem, a characteristic based categorizer client subsystem and a characteristic based categorizer gateway subsystem.

4

[0027] The categories mismatch detector is preferably selected from a set consisting of: a categories mismatch detector server subsystem, a categories mismatch detector client subsystem and a categories mismatch detector gateway subsystem.

[0028] The digital object classifier is preferably selected from a set consisting of: a digital object classifier server subsystem, a digital object classifier client subsystem and a digital object classifier gateway subsystem.

[0029] Further in accordance with a preferred embodiment of the present invention the digital object examiner includes a digital object examiner server subsystem, the characteristics mismatch detector includes a mismatch detector server subsystem and the digital object classifier includes a mismatch detector server subsystem.

[0030] Additionally in accordance with a preferred embodiment of the present invention the digital object examiner includes a digital object examiner gateway subsystem, the characteristics mismatch detector includes a mismatch detector gateway subsystem and the digital object classifier inlcudes a mismatch detector gateway subsystem.

[0031] Preferably, the digital object examiner is selected from a set consisting of: a digital object examiner server subsystem, a digital object examiner client subsystem and a digital object examiner gateway subsystem.

[0032] The digital characteristics mismatch detector is preferably selected from a set consisting of: a characteristics mismatch detector server subsystem, a characteristics mismatch detector client subsystem and a characteristics mismatch detector gateway subsystem.

BRIEF DESCRIPTION OF THE DRAWINGS

[0033] The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawing in which:

Fig. 1 is a simplified pictorial and symbolic illustration of a message bearing an attachment, which contains malicious content;

Figs. 2A, 2B and 2C are simplified pictorial and symbolic illustrations of a preferred embodiment of the functionality of Fig. 1, wherein an e-mail attachment is

5

examined to determine at least two characteristics thereof and analyzing the at least two characteristics to determine whether there exists a mismatch therebetween;

Fig. 3 is a simplified pictorial and symbolic illustration of classifying a file containing a mismatch as a file possibly containing malicious content;

Figs. 4A and 4B are simplified illustrations of comparison of various combinations of more than two characteristics of a file in accordance with a preferred embodiment of the present invention; and

Fig. 5A, 5B and 5C are simplified block diagrams illustrating three embodiments of a system carrying out the functionality of Figs. 1 - 4B.

Fig. 6A, 6B and 6C are simplified block diagrams illustrating yet another three embodiments of a system carrying out the functionality of Figs. 1 - 4B.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

[0034]   Reference is made to Fig. 1, which is a simplified pictorial and symbolic illustration of treatment of a message bearing an attachment which contains malicious content in accordance with a preferred embodiment of the present invention.

[0035]   As seen in Fig. 1, a message 10 bearing an attachment 12 which contains malicious content is symbolized by a message having an attachment indicating icon 14, which appears as a wolf wearing a sheep face mask. In accordance with the present invention, the attachment 12 is scrutinized so as to discern that it contains malicious content, e.g. the sheep face is not the face of a sheep but rather a mask hiding a wolf. Such an attachment is discarded and is not allowed to damage a computer 16 or communication system, as symbolized by the illustrated transfer of the attachment to a wastebasket 18

[0036]   It is appreciated that the present invention is not limited to malicious content in the form of or as part of an e-mail attachment but applies equally to malicious content appearing in any digital object, such as, for example, a file or a web page downloaded from the Internet, a file copied from a diskette or other storage medium or other structured digital object, and to determine the existence of such malicious content by observing a mismatch between at least two characteristics thereof.

[0037]   Reference is now made to Figs. 2A, 2B and 2C which are simplified pictorial and symbolic illustrations of a preferred embodiment of the functionality of

Fig. 1, wherein an e-mail attachment is examined to determine at least two characteristics thereof and analyzing the at least two characteristics to determine whether there exists a mismatch therebetween.

[0038]   As seen in Fig. 2A, an e-mail attachment containing malicious content is symbolized by a wolf wearing a sheep face mask approaching the gate of a fenced-in meadow, which symbolizes a computer network.

[0039]   Fig. 2B shows the wolf wearing a sheep face mask being inspected by a shepherd prior to being allowed to enter the meadow, which corresponds to inspection of the e-mail attachment by the functionality of Fig. 1. The shepherd inspects at least two separate characteristics of the putative sheep, here the face and the tail, corresponding to two separate characteristics of the e-mail attachment, such as the icon and file name extension.

[0040]   The shepherd notices that the inspected characteristics do not match each other, i.e. the putative sheep has the face of a sheep and the tail of an animal other than a sheep. This indicates to the shepherd that something is amiss and he denies the putative sheep access to the meadow, as seen in Fig. 2C, representing discarding the e-mail attachment.

[0041]   Alternatively or additionally, the shepherd may lock up the putative sheep in a corral, which represents a restricted directory, or may issue a visible and/or audio warning, symbolized by blowing on a horn and by smoke signals.

[0042]   Reference is now made to Fig. 3, which is a simplified pictorial and symbolic illustration of classifying a file containing a mismatch as a file possibly containing malicious content. As seen in Fig. 3, at least two of the following characteristics are inspected for the existence of a mismatch therebetween:

e-mail attachment icon 20;

e-mail attachment name extension 22;

e-mail attachment header 24; and

file content 26.

[0043]   Reference is now made to Figs. 4A and 4B are simplified illustrations of comparison of various combinations of more than two characteristics of a file in accordance with a preferred embodiment of the present invention.

7

[0044] Fig. 4A illustrates a situation wherein the e-mail attachment icon 28, the e-mail attachment name extension 30 and the e-mail attachment header 32 all match each other. This indicates the absence of malicious content.

[0045] Fig. 4B illustrates a situation wherein the e-mail attachment icon 34 and the e-mail attachment header match 36 each other, but do not match the e-mail attachment name extension 38. This indicates the presence of malicious content.

[0046] Reference is now made to Fig. 5A, 5B and 5C, which are simplified block diagrams illustrating three embodiments of a system carrying out the functionality of Figs. 1 - 4B.

[0047] Fig. 5A, which illustrates the system of the present invention in a server environment, shows a system 100 for detecting malicious content which comprises a digital object examiner server subsystem 102, examining at least two characteristics of a digital object 104. A characteristic mismatch detector server subsystem 106 receives an output from the digital object examiner server subsystem 102 and analyzes the at least two characteristics to determine whether there exists a mismatch therebetween.

[0048] A digital object classifier server subsystem 108 receives an output from the characteristic mismatch detector server subsystem 106 and is operative upon determination of the existence of a mismatch for classifying the digital object 104 as a digital object possibly containing malicious content. Subsystem 108 may then send a suitable notification 109, as well as the digital object 104, to a client 110 to whom the digital object 104 was directed. Subsystem 108 may, alternatively or additionally, send a suitable notification 114 to a client 112 from whom the digital object was received. Alternatively or additionally, subsystem 108 may discard the digital object 104.

[0049] Fig. 5B, which illustrates the system of the present invention in a client environment, shows a system 200 for detecting malicious content which comprises a digital object examiner client subsystem 202, examining at least two characteristics of a digital object 204. A characteristic mismatch detector client subsystem 206 receives an output from the digital object examiner client subsystem 202 and analyzes the at least two characteristics to determine whether there exists a mismatch therebetween.

[0050] A digital object classifier client subsystem 208 receives an output from the characteristic mismatch detector client subsystem 206 and is operative upon determination of the existence of a mismatch for classifying the digital object 204 as a

8

digital object possibly containing malicious content. Subsystem 208 may then display a suitable visible notification 210 and/or make a suitable audible notification 212 to the user of the client environment. Subsystem 208 may alternatively or additionally discard the digital object 204.

[0051] Fig. 5C, which illustrates the system of the present invention in a gateway environment, shows a system 300 for detecting malicious content which comprises a digital object examiner gateway subsystem 302, examining at least two characteristics of a digital object 304. A characteristic mismatch detector gateway subsystem 306 receives an output from the digital object examiner gateway subsystem 302 and analyzes the at least two characteristics to determine whether there exists a mismatch therebetween.

[0052] A digital object classifier gateway subsystem 308 receives an output from the characteristic mismatch detector gateway subsystem 306 and is operative upon determination of the existence of a mismatch for classifying the digital object 304 as a digital object possibly containing malicious content. Subsystem 308 may then send a suitable notification 309 to a client 310 and/or a suitable notification 316 to the server 311 to which the digital object 304 was directed. Additionally or alternatively, the subsystem 308 may send the digital object 304 to the server 311. Subsystem 308 may, alternatively or additionally, send a suitable notification 314 to a client 312 and/or a suitable notification 318 to the server 313 from whom the digital object 304 was received. Subsystem 308 may alternatively or additionally discard the digital object 304. Alternatively or additionally, subsystem 308 may prevent the digital object 304 from entering a network 320.

[0053] Reference is now made to Fig. 6A, 6B and 6C, which are simplified block diagrams illustrating yet another three embodiments of a system carrying out the functionality of Figs. 1 - 4B.

[0054] Fig. 6A, which illustrates the system of the present invention in a server environment, shows a system 400 for detecting malicious content which comprises a digital object observer server subsystem 402, observing at least two characteristics of a digital object 404. A characteristic based categorizer server subsystem 405 receives an output from the digital object observer server subsystem 402 and analyzes each one of the at least two characteristics in order to categorize the digital object in a category,

9

such as a file type, indicated by that characteristic. A category mismatch detector server subsystem 406 receives an output from the characteristic based categorizer server subsystem 405 and compares the various categories indicated by the various characteristics in order to determine whether there exists a mismatch between the categories.

[0055]   A digital object classifier server subsystem 408 receives an output from the category mismatch detector server subsystem 406 and is operative upon determination of the existence of a category mismatch for classifying the digital object 404 as a digital object possibly containing malicious content. Subsystem 408 may then send a suitable notification 409 to a client 410 to whom the digital object 404 was directed. Subsystem 408 may, alternatively or additionally, send a suitable notification 414 to a client 412 from whom the digital object was received. Alternatively or additionally, subsystem 408 may discard the digital object 404.

[0056]   Fig. 6B, which illustrates the system of the present invention in a client environment, shows a system 500 for detecting malicious content which comprises a digital object observer client subsystem 502, examining at least two characteristics of a digital object 504. A characteristic based categorizer client subsystem 505 receives an output from the digital object observer client subsystem 502 and analyzes any one of the at least two characteristics to determine a category characteristic, such as a file type, of the digital object according to any one of the at least two examined characteristics. A category mismatch detector client subsystem 506 receives an output from the characteristic based categorizer client subsystem 505 and analyzes the determined category characteristics to decide whether there exists a mismatch therebetween.

[0057]   A digital object classifier client subsystem 508 receives an output from the category mismatch detector client subsystem 506 and is operative upon determination of the existence of a mismatch for classifying the digital object 504 as a digital object possibly containing malicious content. Subsystem 508 may then display a suitable visible notification 510 and/or make a suitable audible notification 512 to the user of the client environment. Subsystem 508 may alternatively or additionally discard the digital object 504.

[0058]   Fig. 6C, which illustrates the system of the present invention in a gateway environment, shows a system 600 for detecting malicious content which

10

comprises a digital object observer gateway subsystem 602, examining at least two characteristics of a digital object 604. A characteristic based categorizer gateway subsystem 605 receives an output from the digital object observer gateway subsystem 602 and analyzes any one of the at least two characteristics to determine a category characteristic, such as a file type, of the digital object according to any one of the at least two examined characteristics. A category mismatch detector gateway subsystem 606 receives an output from the characteristic based categorizer gateway subsystem 605 and analyzes the determined category characteristics to decide whether there exists a mismatch therebetween.

[0059]   A digital object classifier gateway subsystem 608 receives an output from the category mismatch detector gateway subsystem 606 and is operative upon determination of the existence of a category mismatch for classifying the digital object 604 as a digital object possibly containing malicious content. Subsystem 608 may then send a suitable notification 609 to a client 610 and/or a suitable notification 616 to the server 611 to which the digital object was directed. Subsystem 608 may, alternatively or additionally, send a suitable notification 618 to a client 612 and/or a suitable notification 620 to a server 613 from whom the digital object 604 was received. Additionally or alternatively, the subsystem 608 may send the digital object 604 to the server 611, which may then pass the digital object 604 to the client 610. Subsystem 608 may, alternatively or additionally, discard the digital object 604. Alternatively or additionally, subsystem 608 may prevent the digital object 604 from entering a network 622.

[0060]   It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the present invention includes both combinations and subcombinations of the various characteristics described hereinabove as well as variations and modifications which would occur to persons skilled in the art upon reading the specification and which are not in the prior art.